FINAL REPORT ON

THE BUREAU OF THE PUBLIC DEBT'S

CHANGE CONTROL PROCEDURES

OIG-00-122 September 15, 2000

This report has been reviewed for public dissemination by the Office of Counsel to the Inspector General. Information requiring protection from public dissemination has been redacted from this report in accordance with the Freedom of Information Act, 5 U.S.C. section 552.

Office of Inspector General

****

United States Department of the Treasury

OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 15, 2000

MEMORANDUM FOR VAN ZECK, COMMISSIONER
BUREAU OF THE PUBLIC DEBT

FROM: Dennis S. Schindel
Assistant Inspector General for Audit

SUBJECT: Final Report on the Bureau of the Public Debt's Change Control Procedures

This memorandum transmits our final report on the Bureau of the Public Debt's Change Control Procedures. This audit was identified as a priority area in the Office of Inspector General's Annual Audit Plan for Fiscal Year 2000. For this audit, we evaluated the Department of the Treasury's change management controls over information system applications, mainframe hardware, and system software at the Bureau of the Public Debt (BPD).

Our audit disclosed activities and procedures that we evaluated as "best practices." In particular, we regard BPD's use of a change control software program for greater change control assurance as a "best practice." Additionally, the high degree of coordination and interaction between the various business units within BPD helps ensure a thorough review of changes prior to their implementation.

Our audit also disclosed deficiencies that could impair BPD's efforts to ensure that only adequately tested and properly approved software is moved into a production environment. Specifically, we noted that not all BPD divisions were using standard testing procedures. We also noted that not all BPD divisions were retaining test documentation and therefore, were unable to demonstrate that all new software changes were tested before being migrated to the production environment.

In our report, we are recommending that BPD: (1) create standard test procedures at both the unit and system acceptance level; and (2) maintain test documentation for 1 year following implementation of changes.

In its response, BPD agreed with our recommendations, and has initiated and planned actions to address the recommendations. BPD's comments have been incorporated into the report and are included in their entirety as Appendix I to the report.

We appreciate the courtesies and cooperation provided to our staff during the audit. If you wish to discuss this report, you may contact me at (202) 927-5400, or a member of your staff may contact Clifford H. Jennings at (202) 927-5771.

Attachment

cc: Chris Testa
Manager, Planning and Research Branch

EXECUTIVE DIGEST

Overview

Weaknesses in the Department of the Treasury's (Treasury) automated information systems change management controls have been identified and reported in Office of Inspector General (OIG) financial statement audit reports. Due to the recurring and Treasury-wide nature of these weaknesses, a change control audit was included in the OIG's Annual Audit Plan for Fiscal Year (FY) 2000. The overall objective of this audit was to determine the adequacy and effectiveness of the Bureau of the Public Debt's (BPD) systems of controls over application, mainframe hardware, and systems software changes.

In this report, we have detailed our evaluation of the change control program at BPD. The report notes activities that we consider instrumental in allowing BPD to achieve repeatable successes in the area of change control. We have also noted deficiencies in BPD's change control program and have made recommendations to help resolve these conditions.

Audit Results

Overall, we found that the change control program at BPD was effective. In particular, BPD's use of a change control software product and extensive internal coordination of changes are examples of strong change management controls. However, in addition to revalidating a previous U.S. General Accounting Office (GAO) finding concerning multiple change management reporting systems, we found two instances where BPD's change control procedures could be improved. In particular:

- BPD was not using standard test plans for unit and system acceptance testing of software changes.

- BPD lacked documentation that software was adequately tested to support the approval for migration to a production environment.

EXECUTIVE DIGEST

Recommendations and Management's Response

We recommend that the Commissioner of BPD should ensure that:

- BPD create and use test plans to ensure that software changes undergo both unit and system acceptance testing before being migrated into production.

- BPD maintain test documentation for 1 year following implementation of changes.

BPD's response to our draft report concurred with our findings and recommendations. Their response is summarized and evaluated in the body of this report and included in detail as Appendix 1, Management Response.

TABLE OF CONTENTS

EXECUTIVE DIGEST

INTRODUCTION

Background 1

Objective, Scope and Methodology 1

AUDIT RESULTS

Overview 2

Details 3

Recommendations 5

APPENDICES

Appendix 1:

Management Response 7

Appendix 2:

Abbreviations 8

Appendix 3:

Major Contributors to this Report 9

Appendix 4:

Report Distribution 10

INTRODUCTION

Background

An adequate and effective change control process ensures that modifications to the computing environment are authorized and tested. Establishing controls over the modification of application software programs and hardware helps to ensure that only authorized programs and authorized modifications (to both hardware and software) are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure that all programs, program modifications and hardware additions are properly authorized, tested, and approved. An additional area of change control is to ensure that access to, and distribution of programs is carefully controlled.

Objective, Scope, and Methodology

The overall objective of this audit was to determine the adequacy, effectiveness, and efficiency of BPD's systems of controls over application, mainframe hardware, and systems software changes. This objective was accomplished by reviewing: (1) system development life cycle methodologies to ensure that the change control process was adequately documented; (2) new and revised software, new hardware installations, and hardware upgrades to determine if they were tested and approved; and (3) whether software libraries exist to provide controls and security against loss or unauthorized access. We also reviewed GAO and OIG audit workpapers developed during reviews of information technology (IT) controls performed in support of FY 1998 and 1999 financial statement audits.

Our fieldwork included reviewing emergency, system software, and mainframe hardware changes. We also reviewed software modifications to BPD's Savings Bond Replacement System (SaBRe) and the Public Debt Accounting and Reporting System (PARS) applications. This report details the fieldwork we performed at BPD [redacted] during March 2000, in accordance with accepted *Government Auditing Standards* and included such audit tests as were determined necessary.

AUDIT RESULTS

Overview

Overall, we found that the change control program at BPD was effective. One of the positive features of this program is BPD's use of a change control software product to control and automate the movement and distribution of software from test through production environments. This product also maintains a history of software versions or modifications, and restricts who can move software into test and production environments.

Another positive feature of BPD's change control program is its formal change management process. This process includes a change management coordinator with review and approval input from representatives of the various parts of the BPD organization, including user groups, programmers, operations, telecommunications, etc. BPD's change control process also includes weekly meetings, reports, follow-up emails, and posted schedules.

Additionally, the Computer Automation, Technology and Security Branch (CATS) has a documented change control methodology that ensures that tested and approved changes are migrated into a production environment. CATS includes system acceptance testing of PARS to ensure that the new modification does not affect the functionality of the system as a whole. We also noted that the system acceptance testing performed by CATS of PARS changes was methodical, documented, and based upon the Change Control for the Public Debt Accounting and Reporting System Manual. This manual includes the requirements for system acceptance testing and updating system documentation.

When we reviewed selected PARS changes, we found all had documentation of testing and approvals. CATS staff stated in interviews that their procedures not only ensure that changes perform as required without a loss of functionality, but that the procedures expedite the training of new employees and the upward mobility of current employees.

AUDIT RESULTS

During our audit fieldwork, we verified the previous GAO finding concerning the use of several different systems to track changes had not yet been corrected. We also found two instances where BPD's change control procedures could be improved. In particular:

- BPD was not using standard test plans for unit and system acceptance testing of software changes.

- BPD lacked documentation that software was adequately tested and to support the approval for migration to a production environment.

Finding

BPD Was Unable to Verify That Software Was Adequately Tested And Properly Approved Prior To Being Moved Into Production

Our review disclosed deficiencies that could impair BPD's efforts to ensure that only adequately tested and properly approved software is moved into a production environment. Specifically, BPD had not ensured that program modifications were adequately tested using standard test plans before the changes were migrated into production. BPD had also not required the retention of documentation of testing performed on these changes. Without documentation of tests performed, we were unable to verify that the changes had been adequately tested.

Details

BPD's Division of Systems Development (DSD) personnel responsible for approving the migration of the SaBRe and PARS changes from the development to the test environment were not relying on the use of standard test plans or test scripts to verify that the new or modified software performed as required without a loss of functionality. BPD's Customer Service and Current Income Branch (CSCIB), which is responsible for system acceptance testing of SaBRe changes before these modifications are moved into production, also did not use standard tests to ensure the modifications performed as requested, or that the system had not lost some functionality due to the change.

Additionally, when we reviewed three randomly selected SaBRe and three PARS changes, we noted that DSD was not retaining documentation of testing performed on modifications to SaBRe and PARS after the changes had been migrated into production. We also determined that CSCIB was not using the SaBRe Systems Analysis Checklist and was not retaining SaBRe testing documentation after the changes had been migrated into production.

The OIG also verified GAO's findings that BPD's change control procedures could be improved. In particular, GAO had noted that there were different tracking systems in use at BPD to manage changes to these applications. The GAO had also found that BPD's Division of Systems Development Handbook did not require formal approvals of program changes nor the retention of test plans and results.

It should be noted that the DSD staff are all BPD employees, not contractors. They have extensive involvement with, and an understanding of both the SaBRe and PARS applications. During fieldwork, we observed that DSD staff made recommendations for corrections and modifications to be included with changes based on their understanding of the software. While it is our judgment that DSD staff are performing adequate tests before migrating the current software from the development to the test environment, we were not able to document this conclusion.

CSCIB staff are also BPD employees, not contractors. They have extensive involvement with, and an understanding of SaBRe. We noted that CSCIB would sometimes assume that new SaBRe changes were ready to go into production without testing due to CSCIB's close working relationship with DSD staff, and the high regard CSCIB had for DSD's capabilities.

However, the applications are becoming more complex, new applications are being developed, and there will be personnel changes. Without a more structured approach to the testing process, including the retention of test documentation, the risk increases that applications will suffer a loss of functionality. Additionally, without test documentation, there is no support for the decision to approve migrating the changes to production.

Treasury Directive Handbook (TD-P 84-01) Information System Life Cycle Manual requires the use of standardized test plans and the use of test documentation for deficiency correction. Additionally, the DSD Division of System Development Handbook requires the use of test plans. CSCIB also has a SaBRe Production and Operating Process Handbook that contains a SaBRe System Analysis Checklist. This checklist requires test plans and documentation.

Recommendations

The Commissioner of BPD should ensure that:

- BPD create and use test plans to ensure that software changes undergo both unit and system acceptance testing before being migrated into production.

  Management Response:

  BPD agreed that, as software is moved from development to a test environment, system test plans and scripts should be used and retained. Because of the early developmental nature of unit testing and its execution by the developer, BPD has taken a less formal approach to unit testing documentation. Since completion of the on-site audit, the DSD has implemented a form where programmers acknowledge that unit testing was performed and briefly describe what was done.

  OIG Comment:

  The OIG agrees that the formal steps BPD has taken and plans to take will provide for a stronger change control environment.

- BPD maintain test documentation for 1 year following implementation of changes.

  Management Response:

  BPD agreed with our recommendation, and recently circulated a Bureau policy memo that requires the retention of test documentation for 2 years. In addition, the DSD procedures have been updated to include the 2 year retention requirement.

  OIG Comment:

  The OIG agrees that the formal steps BPD has taken and plans to take will provide for a stronger change control environment.

Management Response

DEPARTMENT OF THE TREASURY
BUREAU OF THE PUBLIC DEBT
WASHINGTON, DC 20239-0001

August 29, 2000

Memorandum To: Dennis S. Schindel
Assistant Inspector General for Audit

From: Van Zeck, Commissioner
Bureau of the Public Debt

Subject: Draft Audit Report: Review of the Bureau of the Public Debt's Change Control Procedures

In response to your July 14, 2000 draft audit report, the following comments are offered:

FINDING: **BPD was unable to verify that software was adequately tested and properly approved prior to being moved into production.**

RECOMMENDATION: **The Commissioner of BPD should ensure that BPD create and use test plans to ensure that software changes undergo both unit and system acceptance testing before being migrated into production.**

We agree that, as software is moved from development to a test environment, system test plans and scripts should be used and retained. Because of the early developmental nature of unit testing and its execution by the developer, Public Debt has taken a less formal approach to unit testing documentation. Since the completion of the on-site audit, the Division of System Development (DSD) has implemented a form, where programmers acknowledge that unit testing was performed and briefly describe what was done.

RECOMMENDATION: **The Commissioner of BPD should ensure that BPD maintains test documentation for one year following implementation of changes.**

Public Debt agrees with your recommendation, and recently circulated a bureau policy memo that requires the retention of test documentation for two years. In addition, DSD procedures have been updated to include the two year retention requirement.

In closing, we would like to express our appreciation for the positive comments about Public Debt operations which were stated in the draft report.

www.publicdebt.treas.gov

ABBREVIATIONS

BPD	The Bureau of the Public Debt
CSCIB	Customer Service and Current Income Branch
CATS	Computer Automation, Technology and Security Branch
DSD	Division of Systems Development
FY	Fiscal Year
GAO	U.S. General Accounting Office
IT	Information Technology
OIG	Office of Inspector General
PARS	Public Debt Accounting and Reporting System
SaBRe	Savings Bond Replacement System
Treasury	The Department of the Treasury

MAJOR CONTRIBUTORS TO THIS REPORT

Office of Audit

Clifford H. Jennings, Director, Office of IT Audits
Ed Coleman, Deputy Director, Office of IT Audits
Joseph Maranto, IT Lead Auditor
Roger Dressler, IT Audit Manager
Kevin Burke, IT Auditor
Michael Stein, Referencer

REPORT DISTRIBUTION

Bureau of the Public Debt

Office of the Assistant Commissioner for Information Management/Chief Information Officer
Manager, Planning and Research Branch

Treasury Departmental Offices

Office of the Deputy Assistant Secretary for Information Systems/Chief Information Officer
Office of Accounting and Internal Control

Office of Management and Budget

Office of Inspector General Budget Examiner